From 'WarGames' to Aaron Swartz: How U.S. anti-hacking law went astray

Declan McCullagh Former Senior Writer ⋮ 13-17 minutes

The 1983 movie "WarGames" led to an anti-hacking law with felony penalties aimed at deterring intrusions into NORAD. Over time, it became broad and vague enough to ensnare the late Aaron Swartz.

Declan McCullagh is the chief political correspondent for CNET. You can e-mail him or follow him on Twitter as declanm. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.

Aaron Swartz, the Internet activist who committed suicide while facing the possibility of a felony criminal conviction, was prosecuted under a law that was never intended to cover what he was accused of doing.

The Computer Fraud and Abuse Act of 1984 dealt only with bank and defense-related intrusions. But over the years, thanks to constant pressure from the U.S. Department of Justice, the scope of the law slowly crept outward.

So by the time Swartz was arrested in 2011, the tough federal statute meant to protect our national defense secrets covered everything from Bradley Manning's offenses to violating a Web site's terms of use, a breathtaking expansion that has led to a House of Representatives hearing today and other calls for reform.

In the hands of aggressive federal prosecutors, that wide-ranging law has become the proverbial hammer where a scalpel will do. It has been used against a New Jersey man who will be sentenced Monday for accesssing a portion of AT&T's Web site that was not password protected, and against a Missouri woman accused of lying on her MySpace profile.

"In 20 years, we've seen the law become broader and the penalties become more Draconian," says Hanni Fakhoury, a former federal public defender who's now an attorney at

the Electronic Frontier Foundation in San Francisco. "And as a result, we have this situation."

It was the mighty CFAA that brought down Swartz. The district attorney for Massachusetts' Middlesex County, which includes MIT's Cambridge campus, reportedly had no plans to throw the book at him. The curators of the academic database he accessed, JSTOR, have said for years that they had "no interest in this becoming an ongoing legal matter."

But once his case was in federal hands, Swartz became, in the words of prosecutor Carmen Ortiz, no different than a violent criminal. "Stealing is stealing whether you use a computer command or a crowbar," Ortiz said at the time.

What Ortiz didn't say is that the CFAA's punishments, drafted during a post-WarGames computer hacking scare and designed to deter intrusions into NORAD, threatened Swartz with stiffer penalties than if he had been convicted of assault with an actual crowbar. An additional indictment Ortiz's office filed last year sought up to 50 years of prison, which, realistically, meant something like 7 years because Swartz had no criminal record. Justice Department statistics (PDF) show that the median length of incarceration for sexual assault and aggravated assault is 5 years.

A House of Representatives report called WarGames, starring Matthew Broderick and Ally Sheedy, a "realistic representation of the automatic dialing and access capabilities of the personal computer." MGM/United Artists

That disparity stems from the original purpose of the CFAA: to lock up, for a very long time, extremely destructive hackers who might try to disrupt the banking system or tunnel into the U.S. military's classified mainframes.

"WarGames" inspired these extra-long prison terms. As soon as it was released in June 1983, the movie, starring Matthew Broderick as a teenage hacker who broke into NORAD's mainframe and nearly ignited World War III, electrified Capitol Hill and kicked off an anti-hacker panic.

No fewer than six different anti-hacking bills were introduced that year, and Congress convened its first hearings as soon as politicians returned from their summer recess. Rep. Dan Glickman, a Kansas Democrat, opened the proceedings by saying: "We're gonna show about four minutes from the movie 'WarGames,' which I think outlines the problem fairly clearly." A House committee report solemnly intoned: "'WarGames' showed a realistic representation of the automatic dialing and access capabilities of the personal computer."

"WarGames," the first movie to profile hacking so prominently, spilled over into unrelated discussions about national security: a biography of Ronald Reagan recounts how the president asked a group of Democratic congressmen meeting at the White House to discuss arms reduction if they had watched the movie. Rep. Vic Fazio, a California Democrat, recalled Reagan saying: "I don't understand these computers very well, but this young man obviously did. He had tied into NORAD!"

The criminal penalties in those 1983-era bills were primarily aimed at shielding key federal mainframes like NORAD's: one pair of House and Senate measures was titled the "Federal Computer Systems Protection Act of 1983." The witnesses, including representatives of the Defense Department's Computer Security Center, Los Alamos National Lab, and the Treasury Department, were chosen to highlight the threat posted to government computers. A forthcoming book called Cached: Decoding the Internet in Global Popular Culture, by communications professor Stephanie Schulte, says "the release of the film 'WarGames' helped merge Cold War anxieties with those involving teenaged rebellion."

President Reagan, who signed the Computer Fraud and Abuse Act into law in 1984, brought up WarGames during a discussion with members of Congress about arms control. Getty Images

Adding to the concerns of Washington officialdom was that actual hackers called The 414s had recently penetrated the security of banks, manufacturers, and Los Alamos, home to classified nuclear weapon research. Neal Patrick, a 17-year-old student who had been using his family's TRS-80 Model 2 to tunnel into those computer systems, was flown to D.C. to testify that fall. (Patrick had received immunity in exchange for telling the government how

the intrusions took place.)

Prosecutors and politicians quickly became convinced that "WarGames" could become reality. "That movie had a significant effect on my treatment by the federal government," hacker-turned-author Kevin Mitnick told Wired magazine a few years ago. "I was held in solitary confinement for nearly a year because a prosecutor told a judge that if I got near a phone, I could dial up NORAD and launch a nuclear missile."

President Reagan signed the anti-hacking measure, known as the Counterfeit Access Device and Computer Fraud and Abuse Act, into law the following year as part of a broader appropriations bill.

Then, in small but important increments, Congress expanded the CFAA at least nine times over the next few decades at the urging of the Justice Department -- without contemplating how the amendments might eventually sweep in normal activities on the 21st century Internet. A 1986 addition punished schemes to defraud through computers. In 1994, Congress made CFAA violations a civil offense, opening the door to private litigation. Another change, in 1996, replaced the language "federal interest computer" with revised wording that applied to every computer in the United States.

In 2001, the USA Patriot Act rewrote the CFAA to make it easier for prosecutors to allege felonies. It also doubled the maximum punishment for first-time offenders such as Swartz. In 2002, a little-known section of the bipartisan law creating the Department of Homeland Security led the U.S. Sentencing Commission, defaced earlier this year by pro-Swartz hackers, to stiffen penalties (PDF) for violations still more.

"The Department of Justice is kind of phobic in this area," says Harvey Silverglate, author of Three Felonies a Day and a criminal defense attorney in Cambridge who first met Swartz in 2001. "Phobia and panic has really led to, I think, a lot of the overuse and the abusive use of the CFAA. There's enough vagueness in the CFAA that it really can be stretched -- and of course that's what happened in Aaron's case."

Hacker-turned-author Kevin Mitnick after being released from the Federal Correctional Institution in Lompoc, Calif., in 2000. Getty Images

Over time, Congress' tinkering with the CFAA produced a potent weapon that allowed prosecutors to threaten defendants with extremely long prison sentences. Mitnick, perhaps the world's most famous computer hacker, spent five years in prison in the 1990s despite a previous criminal conviction and years as a fugitive. Nearly two decades later, Swartz faced a likely seven-year sentence from a more muscular CFAA and a trial set to begin in April before Judge Nathaniel Gorton, a George H.W. Bush appointee with a reputation as a tough judge and a tough sentencer, who could easily levy a stiffer penalty than even prosecutors were seeking.

"The extraordinary potential sentences are a result of political pressure by the Department of Justice, characteristic of their pressing for higher penalties in all sorts of areas of criminal regulation," says Jennifer Granick, director of civil liberties at the Stanford Center for Internet and Society, who has represented hackers facing criminal charges.

The Justice Department has not been shy in wielding the CFAA aggressively. Lori Drew, a Missouri woman who the department charged with not complying with MySpace's terms of service, was convicted by a federal jury of misdemeanor violations of the CFAA. A federal judge eventually overturned the guilty verdict, but only on a technicality because it was a misdemeanor conviction. Ironically, if the jury had decided more serious felony charges were appropriate, U.S. District Judge George Wu said at the time, the conviction would have remained intact.

Instead of trying to fix the CFAA by excluding terms of service violations, the Obama administration has veered in the opposite direction. In 2011, the White House proposed additions it described as (PDF) enhancing "the criminal penalties," inserting additional types of violations, and punishing some CFAA-related offenses as criminal racketeering under a 1970 law intended to target organized crime. The Center for Democracy and Technology warned at the time that, under President Obama's plan (PDF), someone who jailbreaks his

iPad and "shares with others the code that he used to gain access" would become "subject to criminal penalty."

That nearly became law. Vermont Sen. Patrick Leahy incorporated the administration's request into a bill backed by the Justice Department and other Democrats including Connecticut's Richard Blumenthal and New York's Chuck Schumer. Like the earlier expansions, it was endorsed by the Justice Department: James Baker, deputy attorney general, predicted it will ensure that "cybercrime is deterred effectively and punished appropriately." Treating certain CFAA violations as racketeering "strikes me as appropriate here," Baker said.

Leahy's proposal, called the Personal Data Privacy and Security Act, was approved by the Senate Judiciary committee in November 2011 with some amendments, but then stalled. Undaunted, Leahy tried again last summer by proposing similar CFAA-strengthening language as an amendment to then-senator Joe Lieberman's broader cybersecurity bill.

Leahy's amendment alarmed the ACLU, the National Association of Criminal Defense Lawyers, Grover Norquist's Americans for Tax Reform, and other groups, which had hoped to narrow the CFAA, not expand it. In a letter to Leahy (PDF), they warned that "the CFAA should focus on malicious hacking and identity theft and not on criminalizing any behavior that happens to take place online in violation of terms of service." Lieberman's bill failed on a largely party-line vote in the Senate.

Rep. Zoe Lofgren, a Democrat who represents the heart of Silicon Valley, is trying to fix the Computer Fraud and Abuse Act. Her proposal faces serious hurdles. Getty Images

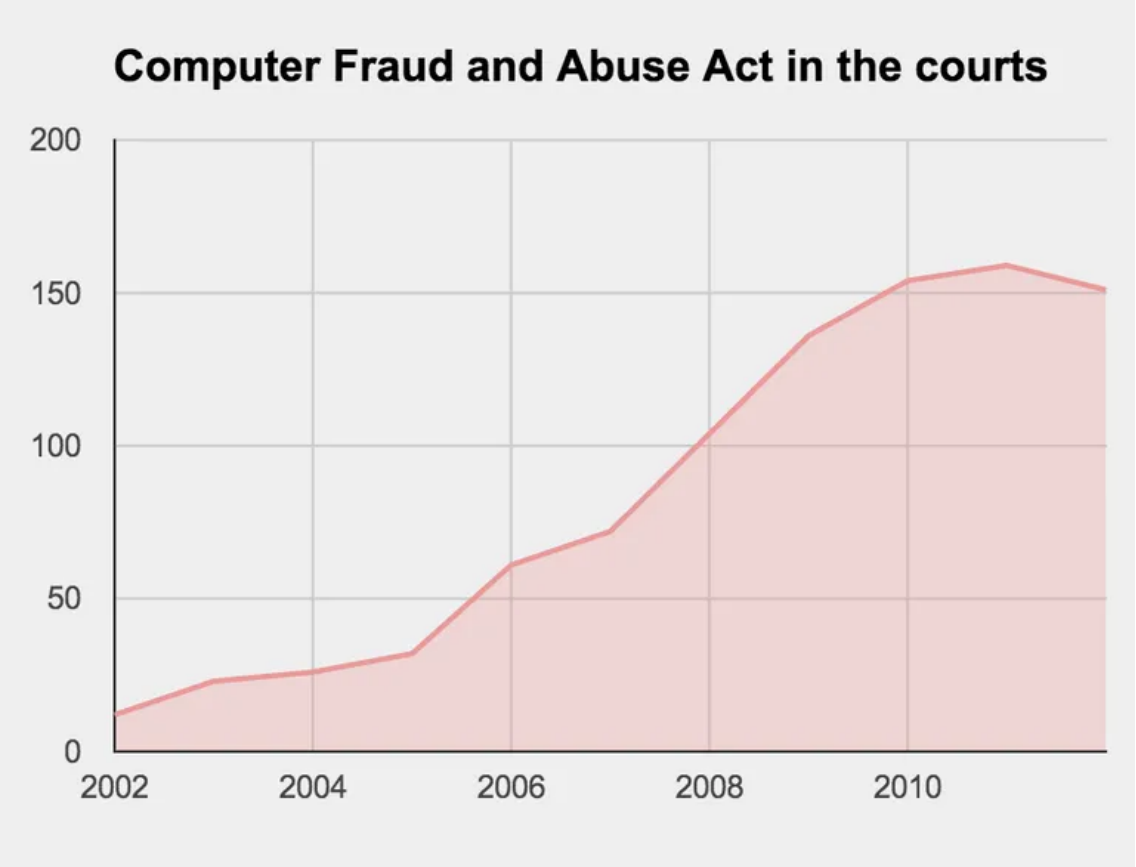
This year, Swartz's suicide months before his criminal trial would have begun has led to unprecedented public interest in details of the CFAA and a flurry of calls for reform. Orin Kerr, a former Justice Department prosecutor and law professor at George Washington University who's expected to testify at today's hearing, has proposed deleting the nebulous language that criminalizes "exceeding unauthorized access." Kerr's written testimony (PDF) says the CFAA is "remarkably vague" and should be amended to "ensure that innocent

conduct is not criminalized."

The Electronic Frontier Foundation has offered its own proposal, as has Rep. Zoe Lofgren, a Democrat from Silicon Valley who has drafted "Aaron's Law." Engine Advocacy and startups including OpenDNS, PadMapper, and Stack Exchange wrote a letter (PDF) yesterday to the House Judiciary committee in support of Lofgren, warning that the CFAA threatens "developers and entrepreneurs who create groundbreaking technology."

But the Justice Department, which declined to comment yesterday, will certainly oppose any such measure. The department has a good track record of enacting legislation it likes, and especially in a political climate influenced by heightened fears of "cyber-attacks," a near-perfect history of derailing legislation it doesn't. Baker, the deputy attorney general, previously warned the Senate Judiciary committee that "proposals to modify the terms of the existing act... would have the unintentional effect of undermining the CFAA."

"I can't recall a time when Congress has ever voted to decrease penalties," says Fakhoury, the EFF attorney. "The law's been expanded, and expanded, and expanded. And now we're in the mess we're in today."



The Computer Fraud and Abuse Act's explosive growth over the last decade: this chart shows the number of times it was cited by federal judges each year in criminal and civil cases. CNET research